DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

Vehicle-to-Vehicle Security Credential Management System; Request for Information

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT).

ACTION: Notice – Request for Information (RFI).

SUMMARY: On August 18, 2014, NHTSA announced an advance notice of proposed rulemaking (ANPRM) for V2V communications, and concurrently released an extensive research report on the technology, as the formal start to the regulatory process. This notice, a Request for Information (RFI), seeks information related to the security system that will support V2V operations but will not be established by NHTSA regulation. This RFI will help the agency: (1) Become aware of private entities that may have an interest in exploring the possibility of developing and/or operating components of a V2V Security Credential Management System (SCMS); (2) Receive responses to the questions posed about the establishment of an SCMS provided in the last section of this RFI; and (3) Obtain feedback, expressions of interest, and comments from all interested public, private, and academic entities on any aspect of the SCMS.

The Background section of this RFI provides an overview of the technical and organizational aspects of the current V2V security design, of which the SCMS is an integral part. The SCMS encompasses all technical, organizational, and operational aspects of the V2V security system that is needed to support trusted, safe/secure V2V communications and to protect driver privacy appropriately. The primary managerial component of the envisioned SCMS

(called the SCMS Manager) would be responsible for managing all other component entities (called Certificate Management Entities or CMEs) which support the different V2V security functions that, together, ensure the operational integrity of the total system.

DATES: Responses to this RFI should be submitted by 11:59 p.m., E.T., on **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Responses: You may submit responses, identified by Docket No. NHTSA-2014-0023, by any of the following methods:

Internet: To submit responses electronically, go to http://www.regulations.gov and follow the online instructions for submitting comments. Alternatively, go to http://www.safercar.gov/v2v/index.html and click the yellow button labeled "Submit responses on the SCMS Request for Information" to go directly to the docket in regulations.gov.

Facsimile: Written responses may be faxed to 1-202-493-2251.

Mail: Send responses to Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue, SE, West Building Ground Floor, Room W12-140, Washington, DC 20590.

Hand Delivery: If you plan to submit written responses by hand or by courier, please do so at U.S. Department of Transportation, 1200 New Jersey Avenue, SE, West Building Ground Floor, Room W12-140, Washington, DC between 9 a.m. and 5 p.m. E.T., Monday through Friday, except Federal holidays. You may call the Docket Management Facility at 1-800-647-5527

FOR FURTHER INFORMATION CONTACT: For questions about the program discussed herein, contact John Harding, NHTSA, Intelligent Technologies Research Division, 202-366-

5665, john.harding@dot.gov. For legal questions, interpretations and counsel, please contact Rebecca Yoon, Office of the Chief Counsel, 202-366-8909, rebecca.yoon@dot.gov, 1200 New Jersey Avenue, SE, Washington, DC 20590.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Purpose of this Notice

NHTSA seeks responses from parties potentially interested in establishing and operating a V2V SCMS. Respondents can express interest, provide comments concerning the establishment of an SCMS, provide information concerning security approaches for a V2V environment, and discuss the technical and organizational aspects of the SCMS. While comments are welcome on any area of the RFI, NHTSA is particularly interested in responses related to interest in establishing an SCMS, including but not limited to some or all of the legally distinct CMEs that make up the SCMS, along with responses to the questions detailed in the Summary of Questions section of this RFI.

II. RFI Guidelines

Responses to this notice are not offers and cannot be accepted by the Government to form a binding contract or issue a grant. Information obtained as a result of this RFI may be used by the Government for program planning on a non-attribution basis. This RFI notice is NOT a solicitation for proposals, applications, proposal abstracts, or quotations. This RFI notice is not to be construed as a commitment on the part of the Government to award a contract or grant, nor does the Government intend to directly pay for any information or responses submitted as a result of this RFI notice.

The Government prefers that submissions NOT include any information that might be considered proprietary or confidential. The Government intends to publicly release a summary of responses to this RFI. Such a summary may identify the number and types of respondents (e.g., public agency, private entity, or academic institution). If you wish to submit any information under a claim of confidentiality, you should submit three copies of your complete submission, including the information you claim to be confidential business information, to the Chief Counsel, NHTSA, at the address given above under **FOR FURTHER INFORMATION CONTACT**. In addition, you should submit two copies, from which you have deleted the claimed confidential business information, to Docket Management at the address given above under **ADDRESSES**. When you send a comment containing information claimed to be confidential business information, you should include a cover letter, as specified in our confidential business information regulation (49 CFR part 512.), that delineates that information.

Responses should clearly identify the name(s) of the responding organization(s) or individual(s) and a designated point of contact, to include address, e-mail, and phone number.

III. Background on V2V and the Agency's Actions Thus Far

The U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) announced on February 3, 2014, that it will begin taking steps to enable vehicle-to-vehicle (V2V) communication technology for light vehicles. This technology would improve safety by enabling nearby V2V devices to "talk" to each other using dedicated short range communication (DSRC) to exchange, up to ten times per second, basic safety data such as speed and position. This data could then be used by vehicles to warn drivers of impending danger from other vehicles, and ultimately could help avoid many crashes altogether.

On August 18, 2014, NHTSA announced an advance notice of proposed rulemaking (ANPRM) for V2V communications, and concurrently released an extensive research report on the technology. The research report contains a comprehensive discussion of the agency's current vision for an SCMS in terms of governance, design, and potential costs. The ANPRM contains a number of SCMS and security-related questions on which the agency is seeking responses, which may also assist those responding to this RFI. Although we provide a brief summary below, NHTSA believes that respondents will be in the best position to respond comprehensively to this RFI if they also review the research report and the questions in the ANPRM. Responses to this RFI will be maximally helpful to the agency if they are focused on the specific issue of commenters' potential interest in operating an SCMS and how they might approach doing so, as well as the other points raised specifically in this RFI. Responses to the RFI will be collected in Docket No. NHTSA-2014-0024. NHTSA requests that respondents who wish to address V2V issues more broadly, including issues those related to SCMS and security beyond what is discussed in this RFI, please comment to the ANPRM and research report at Docket No. NHTSA-2014-0022. The response period for the ANPRM closes on October 20, 2014.

In order to function safely, a V2V system must have trusted communication between V2V devices and message content that is protected from outside interference. In order to create the required environment of trust, a V2V system must include security infrastructure to secure each message, as well as a communications network to convey security and related information from vehicles to the entities providing system security (and vice versa).

During the Connected Vehicle Safety Pilot Model Deployment (i.e., Model Deployment), concluded in the Ann Arbor, MI area in 2013 and 2014, V2V devices installed in roughly 2,800 light vehicles were able to transmit and receive messages from one another using security credentials supplied by a prototype security management system. This system was based on a design jointly developed by DOT and the Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications 3 (VSC3) Consortium, a consortium of eight automobile manufacturers. The security system successfully provided trusted and secure communications among the equipped vehicles deployed for Model Deployment. This was accomplished with relatively few problems given the magnitude of this first-of-its-kind demonstration project.

In the future, however, if the agency mandates V2V communications devices for all new light vehicles, a much larger security infrastructure and communications network would be necessary to provide that required trust. At this point, DOT and NHTSA anticipate that private entities will create, fund, and manage the security and communications components of a V2V system. While NHTSA has identified several potential types of entities that might be interested in participating in a V2V security system, NHTSA has not identified any private entities that have expressed a willingness to do so.

IV. Security Overview and Operational Characteristics

In this section, the agency provides an overview of the discussion of communications security issues associated with V2V, including the nature of the SCMS, as well as a discussion of the agency's legal relationship with a private SCMS system. For a complete discussion of these issues, please see Part IX of the research report.

A. Technical Aspects

In contrast to other types of safety technologies currently widespread, or increasingly present, in the vehicle fleet, safety applications based on V2V are cooperative—meaning that participating vehicles must exchange (i.e. broadcast and receive) and analyze data in real-time. This cooperative exchange of vehicle to vehicle messages, which represents a new opportunity for vehicle safety, supplies the information needed by a vehicle to prepare driver alerts and warnings about potential hazardous situations. It also gives vehicles the ability to use that information to generate information about mobility and environmental conditions, and communicate with road-side infrastructure. However, a cooperative system can only work when participants in the system are able to trust the alerts and warnings issued by their V2V devices that are based, at least in part, upon information received from other V2V devices.

For this reason, a primary requirement for a V2V system is "trust"—a requirement that thousands of data messages will be authenticated, in real-time, as being unaltered and coming from a trusted source. It is also a critical element in achieving "interoperability"— so that vehicles of different make/model/year will be able to talk to each other and exchange trusted data without pre-existing agreements or altering vehicle designs. In furtherance of system-wide trust, a V2V system also needs to be secure against internal and external threats or attacks.

Thus, the three primary elements of the V2V system that require security are the:

- V2V communications (the medium, the messages/data, the certificates, and any other element that supports message exchange);
- V2V devices; and
- V2V security system itself (through organizational, operational, and physical controls).

In addition to these requirements, the V2V system needs to be: (1) ultimately scalable to meet the needs of over 350 million users across the nation (such as light vehicles, heavy vehicles, motorcycles, pedestrians, bicycles, etc.), (2) extendable to accommodate other types of applications (such as V2I mobility, traffic management, and environmental applications), and 3) financially sustainable to ensure its continued operation over time.

In considering which security technologies would most effectively provide trusted message exchange and secure communications for safety-critical applications, DOT and NHTSA, along with CAMP security experts, compared three different security approaches — symmetric encryption, group signature, and asymmetric public key infrastructure (PKI). When assessing these alternatives, the V2V research team was looking for an option that:

- Protects driver privacy appropriately by not requiring participants to disclose their identities;
- Works quickly enough to fit within the bandwidth constraints of DSRC and the expected processing constraints of the V2V on-board equipment;

- Does not require over-the-air bytes for security that exceed the constraints of DSRC bandwidth and size of the Basic Safety Message (BSM) in the message payload; and
- Supports non-repudiation.[1]

After considering the characteristics of each security approach, the research development team preliminarily determined that the PKI option (asymmetric key) using the signature method offered the most effective approach to achieving communications security and trusted messaging for a very large set of users. For this reason, the research team chose that approach to secure the BSM that is at the center of the current V2V system design. Significantly, the effectiveness of this approach is highly dependent upon technical design decisions relating to *how* the approach is deployed in a given environment.

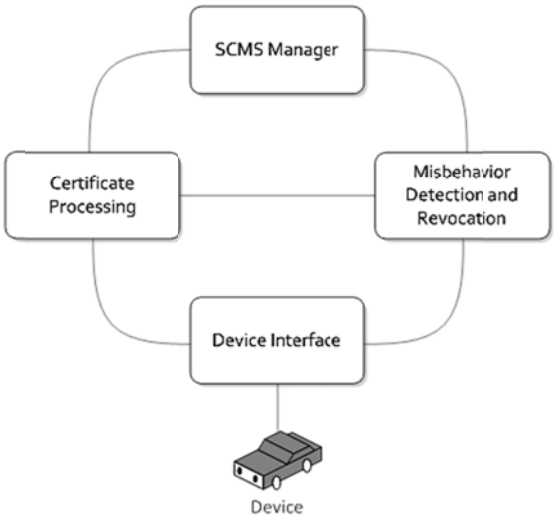
B. V2V security design concept: functions, components, communications

Figure 1 presents the high level, basic components/functions of the V2V security system. They are similar to the basic functions of any Public Key Infrastructure (PKI) security system.

Figure 1 Simplified V2V Security System

[GPO – PHOTO GRAPHIC]

[1] Non-repudiation in public-key technology is traditionally defined as the inability of a person (to whom a public key has been bound by a recognized certification authority through issuance of a public key certificate) to deny having made some digital signature.



[END PHOTO]

For reference, Table 1 contains a list of abbreviations used to describe the system discussed in more detail below:

Table 1 Security Related Acronyms

Acronym	Definition
BSM	basic safety message
CA	certificate authority
CME	certificate management entity
CP	certificate policy
CRL	certificate revocation list
DCA	device configuration manager
ECA	enrollment certificate authority
FIPS	Federal Information Processing Standards
LA	linkage authority
LOP	location obscurer proxy
MA	misbehavior authority
PCA	pseudonym certificate authority
PII	personally identifiable information
PKI	public-key infrastructure
RA	registration authority
SCMS	security credential management system

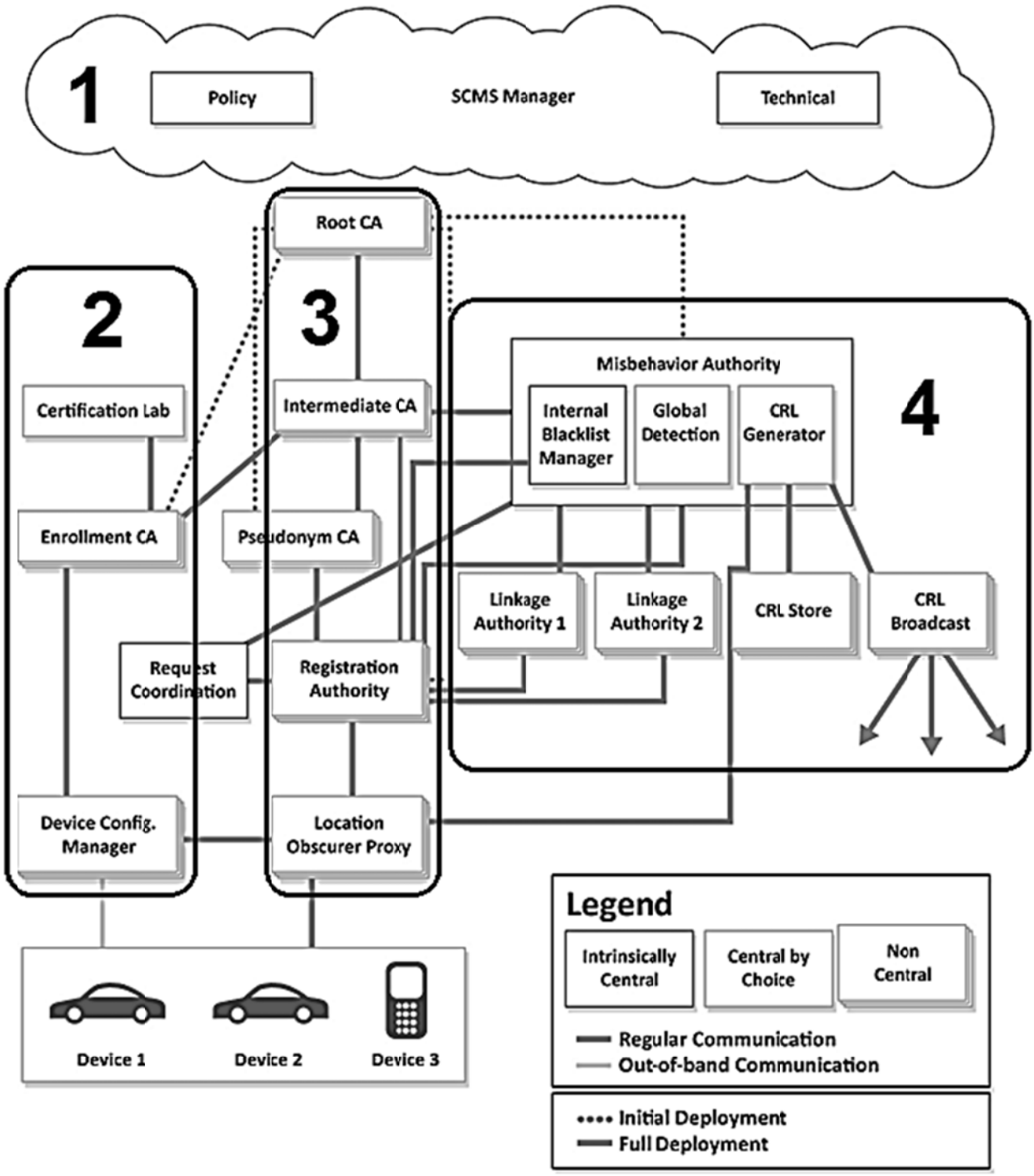
Figure 2 illustrates multiple security and privacy operations and components that DOT envisions for a V2V system to accomplish the distribution of certificates in a way that is trusted

and that protects consumers' privacy. The fundamental operations are indicated as 1) Overall Management, 2) Registration and Enrollment, 3) Certificate Management and 4) Misbehavior Management. The text following this illustration contains definitions for each component.

Figure 2 Current V2V Security System Design for Deployment and Operations[2]

[GPO – PHOTO GRAPHIC]

[2] This image presents both an initial deployment model as well as a full deployment model. Note that this diagram shows the initial deployment model in which there is no Intermediate Certificate Authority (CA) and the Root CA talks to the Misbehavior Authority (MA), Pseudonym Certificate Authority,(PCA) and Enrollment Certificate Authority (ECA) (dotted lines). In the full deployment model, these entities communicate with the Intermediate CA instead of the Root CA to protect the Root CA from unnecessary exposure (solid line).



[END PHOTO]

The following discussion of SCMS functions focuses on communications and activities within the SCMS. The technical design for the SCMS includes several different operating

functions that, together, make up the overall SCMS structure. It is envisioned that single or multiple operating functions will be carried out by individual, legally distinct CMEs (including the SCMS Manager) that, together, will make up the SCMS organization. The agency is interested in respondents providing their views on potential structure of the entire SCMS organization, including the distinction, if one is needed, between separate components and responsibilities.

That said, we note that the interaction between the components shown in Figure 2 is all based on machine-to-machine performance. No human judgment is involved in creation, granting, or revocation of the digital certificates. The functions are performed automatically by processors in the various V2V components, including the vehicle's on-board equipment (OBE). The role of personnel within the SCMS is to manage the overall system, protect and maintain the computer hardware and facilities, update software and hardware, and address unanticipated issues.[3]

Generally, these SCMS operating functions fall into two categories: "pseudonym functions" and "bootstrap functions," discussed further below. In order for the SCMS to support the security needs of the V2V system, the various SCMS functions (housed in different CME organizations) must work together to exchange information securely and efficiently.

C. Pseudonym functions/certificates

The security design employs short-term digital certificates used by a vehicle's V2V device to authenticate and validate BSMs that are sent and received. Since these BSMs provide

[3] The SCMS manager would establish policies and procedures that influence the configuration of the system parameters.

the information needed for V2V-based safety warning technologies to operate, it is important that they are trustworthy. A valid certificate indicates the BSM was transmitted from a trusted source. A BSM with a revoked (invalid) certificate is ignored by other V2V devices. In order to protect privacy appropriately, these short-term certificates do not contain any information about the vehicles and their occupants (e.g., drivers/occupants or vehicle make/model/VIN), but they serve as credentials that permit vehicles to participate in the V2V system.

Pseudonym functions create, manage, distribute, monitor, and revoke short-term certificates for vehicles. They include the following functions:

- Intermediate Certificate Authority (Intermediate CA), which is an extension of the Root CA, shielding it from direct access to the internet. It can authorize other CMEs (or possibly an Enrollment Certificate Authority [ECA]) using authority from the Root CA, but does not hold the same authority as the Root CA in that it cannot self-sign a certificate. The Intermediate CA provides flexibility in the system because it removes the need for the highly protected Root CA to establish contact with every SCMS entity as they are added to the system over time. Additionally, the use of Intermediate CAs lessens the impact of an attack by maintaining protection of the Root CA.
- Linkage Authority (LA), which is the entity that generates linkage values. The LA comes in pairs of two, which we refer to as LA1 and LA2, in order to further protect privacy. The LAs for most operations communicate only with the RA and provide values, known as linkage values, in response to a request by the RA (see below) and PCA (see below). The linkage values provide the PCA with a means to calculate a certificate ID and a mechanism to connect all short-term certificates from a specific device for ease of revocation in the event of misbehavior.

- Location Obscurer Proxy (LOP), which obscures the location of OBE seeking to communicate with the SCMS functions, so that the functions are not aware of the geographic location of a specific vehicle. All communications from the OBE to the SCMS components must pass through the LOP. Additionally, the LOP may shuffle misbehavior reports that are sent by OBEs to the MA (see below) during full deployment. This function increases participant privacy but does not increase or reduce security.
- Misbehavior Authority (MA), which acts as the central function to process misbehavior reports, as well as to produce and publish the certificate revocation list (CRL). It works with the PCA, RA, and LAs to acquire necessary information about a certificate to create entries to the CRL through the CRL Generator. The MA eventually may perform global misbehavior detection, involving investigations or other processes to identify levels of misbehavior in the system. The MA is not an external law enforcement function, but rather an internal SCMS function intended to detect when messages are not plausible or when there is potential malfunction or malfeasance within the system. The extent to which the CMEs share externally information generated by the MA about devices sending inaccurate or false messages – whether with individuals whose credentials the system has revoked, regulatory agencies or law enforcement – will depend on law, organizational policy, and/or contractual obligations applicable to the CMEs and their component functions.
- Pseudonym Certificate Authority (PCA), which issues the short-term certificates used to ensure trust in the system. In earlier designs their lifetime was fixed at five minutes. The validity period of certificates is still on the order of "minutes" but is now a variable length of time, making them less predictable and thus harder to track. Certificates are the

security credentials that authenticate messages (BSM) from a device. In addition to certificate issuance, the PCA collaborates with the MA, RA, and LAs to identify linkage values to place on the CRL if misbehavior has been detected. Individual PCAs may be limited to a particular manufacturer or a particular region.

- Registration Authority (RA), which performs the necessary key expansions before the PCA performs the final ones. It receives certificate requests from the OBE (by way of the LOP), requests and receives linkage values from the LAs, and sends certificate requests to the PCA. It shuffles requests from multiple OBEs to prevent the PCA from correlating certificate IDs with users. It also acts as the final conduit to batching short-term certificates for distribution to the OBE. Lastly, it creates and maintains a blacklist of enrollment certificates so it will know to reject certificate renewal requests from revoked OBEs.

- Request Coordination, which is critical in preventing an OBE from receiving multiple batches of certificates from different RAs. The Request Coordination function coordinates activities with the RAs to ensure that certificate requests during a given time period are responded to appropriately and without duplication. Note that this function is only necessary if there is more than one RA in the SCMS.

- Root Certificate Authority (Root CA), which is the master root for all other CAs; it is the "center of trust" of the system. It issues certificates to subordinate CAs in a hierarchical fashion (as well as MA, LAs and RAs), providing their authentication within the system so all other users and functions know they can be trusted. The Root CA produces a self-signed certificate (verifying its own trustworthiness) using out-of-band communications. This enables trust that can be verified between ad hoc or disparate devices because they

share a common trust point. It is likely that the Root CA will operate in a separate, offline environment because compromise of this function is a catastrophic event for the security system.

- SCMS Manager, which is the function that will provide the policy and technical standards for the entire V2V system. Just as any large-scale industry ensures consistency and standardization of technical specifications, standard operating procedures (SOPs), and other industry-wide practices such as auditing, the SCMS Manager would establish SOPs, including in such areas as interoperability, security, privacy and auditing, and manage the activities required for smooth and expected operation of the SCMS. This could happen in a number of ways. Often in commercial industries, volunteer industry consortia take on this role. In other industries, or in public or quasi-public industries, this role may be assumed by a regulatory or other legal or policy body.

Regardless of how the SCMS "industry" establishes and operates a central administrative body, it is expected that one will be established for the V2V SCMS. As no decisions about ownership or operation have been made, we do not advocate for public or private ownership of the CMEs that will make up the SCMS. Rather, in our discussions and analyses, we identify the basic functions that we expect the SCMS Manager will perform. The expectation is that the CMEs that make up the SCMS, either voluntarily or contractually, will agree to adhere to the SOPs, audit standards, and other practices established by the SCMS Manager. In accordance with input from DOT, the SCMS Manager will develop applicable guidance, practices, SOPs, auditing standards, or additional industry-wide procedures in coordination with, or so as to dovetail with Federal guidance or regulations applicable to V2V communications. NHTSA also

assumes that the CMEs will endow the SCMS manager with authority to remove from the SCMS or revoke the "credentials" of CMEs that misbehave or do not comply with applicable standards.

D. "Bootstrap"/initialization functions/enrollment certificate

The security design also includes functions that carry out the bootstrapping process, which establishes the initial connection between a V2V device and the SCMS. The chief functional component of this process is the Enrollment Certificate Authority (ECA), which assigns a long-term enrollment certificate to each V2V device.

Initialization functions include:

- Certification Lab, which instructs the Enrollment CA on polices and rules for issuing enrollment certificates, i.e. device enrollment criteria. This is usually done when a new device is released to the market or if the SCMS Manager releases new rules and guidelines. The Enrollment CA uses information from the Certification lab to confirm that devices of the given type are entitled to an enrollment certificate. At this time, specific details regarding the Certification and Enforcement are not defined.[4]

- Device Configuration Manager (DCM), which is responsible for giving devices access to new trust information, such as updates to the certificates of one or more authorities, and relaying policy decisions or technical guidelines issued by the SCMS Manager. It also

[4] At this point, the extent and level of testing which the Certification Lab will actually perform is still to be determined. The role of the labs could range from simply managing a checklist of requirements to performing extensive technical certification tests, including: device performance, FCC compliance, cryptographic testing (at the level of FIPS-140), and/or interoperability testing. The intent is that the SCMS Manager, after it is created, will determine the full roles and responsibilities of the Certification Lab. Vehicle and device manufacturers may decide to rely in part on a certification lab to support their own certification of compliance with any relevant standards NHTSA may issue.

sends software updates to devices. The DCM coordinates initial trust distribution with devices by passing on credentials for other SCMS entities, and provides a device with information it needs to request short term certificates from an RA. The DCM also plays a role in the bootstrap process by ensuring that a device is cleared to receive its enrollment certificate from the ECA. It also provides a secure channel to the ECA. There are two types of connections used from devices to the DCM: in-band and out-of-band communications. In-band communication utilizes the LOP, while out-of-band communication is sent directly from the device to the ECA, by way of the DCM.

- Enrollment Certificate Authority (ECA), which verifies the validity of the device type with the Certification Lab. Once verified, the ECA then produces the enrollment certificate and sends it to the OBE. Once the OBE has a valid enrollment certificate, it is able to request and receive certificates from the SCMS. Individual PCAs may be limited to a particular manufacturer or a particular region.

E. Privacy Considerations

Risks to consumer privacy, whether actual or perceived, are intertwined with consumer and industry acceptance of V2V technologies. For this reason, privacy considerations are critical to the analysis underlying NHTSA's decision about how to proceed with regulation.

At the outset, readers should understand some very important points about the V2V system as contemplated by NHTSA. The system will not collect or store any data on individuals or individual vehicles, nor will it enable the government to do so. There is no data in the basic

safety messages broadcast by V2V devices or collected by the V2V security system intended to be used by law enforcement or private entities to personally identify a speeding or erratic driver.[5] The system—presumably operated by private entities—will not permit tracking through space or time of vehicles linked to specific owners or drivers or persons. Third parties attempting to use the system to track a vehicle would find it extremely difficult to do so, particularly in light of far simpler and cheaper means available for that purpose. The system will not collect financial information, personal communications, or other information linked to individuals. It will enroll V2V enabled vehicles automatically, without collecting any information identifying specific vehicles or owners.

The system will not provide a "pipe" into the vehicle for extracting data. While the system needs to enable NHTSA and motor vehicle manufacturers to find lots or production runs in the event of defective and/or non-compliant V2V devices, it will do so without use of VIN numbers or other information that could identify specific drivers or vehicles.

There are two primary categories of V2V system functions that involve the transmission, collection, storage, and sharing of V2V data by, and between, the V2V system components and other entities: system safety and system security.

The V2V system's safety functionality (i.e., the safety applications that produce crash warnings) requires that V2V devices broadcast and receive a basic safety message containing information about vehicle position, heading, speed, and other information relating to vehicle

[5] Definition of the current basic safety message data elements is found in Table V-1 and Table V-2 of the agency's V2V research report, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application V1.0 August, 2014"

state and predicted path. The BSM, however, contains no personally identifying information (PII) and is broadcast in a very limited geographical range, typically less than 1 km. Nearby devices installed in other vehicles will use that information to warn drivers of crash-imminent situations. Except as necessary to identify devices in the case of malfunction, the system will not collect, and motor vehicles will not store, the messages or data that are sent or received by V2V devices.

F. Device non-compliance and potential recalls

Currently, as discussed in the report, NHTSA may need to conduct further research into how to ensure that all V2V devices subject to a recall can be identified, and that owners can be notified about the issue and be provided instructions for how to remedy a potential condition. Section VIII.B.3 of the agency's V2V research report discusses the possibility that for vehicles manufactured with V2V devices installed, the SCMS may be able to create a link at the time of manufacture between specific installed V2V devices or production lots of devices and enrollment certificates that later may help vehicle manufacturers and NHTSA identify defective V2V equipment, potentially linking device batches to enrollment certificates. However, it is not yet clear how such a linkage would be created for V2V devices that are not installed by the manufacturer. The agency welcomes discussion from respondents on the potential approach discussed in the report along with other potential approaches, based on a respondent's experience, which NHTSA may employ to fulfill its defect and non-compliance identification responsibilities.

The security needs of the V2V system require the exchange of certificates and other communications between: (1) V2V devices and (2) the entity or entities providing security for the V2V system (i.e., the Security Credential Management System). These two-way

communications are encrypted and subject to additional security measures. These measures are designed to prevent SCMS insiders and others from unauthorized access to information that might enable linkage of BSM data or security credentials to specific motor vehicles.

NHTSA also needs to ensure that the V2V system is protected from defective and non-compliant devices. In order to do so, the V2V security system will likely need to collect and share with manufacturers, such that they can comply with Federal regulations, on a very limited basis, some V2V data linking V2V device production lots to security credentials. However, as currently envisioned, neither the V2V system nor NHTSA will collect, store, or have access to information that links production lots of defective V2V devices with specific VINs or owners.

NHTSA and the DOT take privacy very seriously. If NHTSA moves forward with regulating V2V technologies, we are committed to doing so in a manner that both protects individual privacy appropriately and promotes this important safety technology.

V. SCMS Organizational Options

The above discussion of SCMS functions focused on activities and communications within the SCMS. The current section discusses the DOT research performed by Booz Allen Hamilton (BAH), with input from CAMP and the Vehicle Infrastructure Integration Consortium (VIIC), on the development of an SCMS organization. The purpose of BAH's research was to generate organizational options for an SCMS capable of enabling secure and efficient communications, protecting privacy appropriately, and minimizing operational costs. BAH developed a number of different organizational options by grouping the SCMS functions in CAMP's design into legally/administratively distinct entities. BAH's analysis of the organizational options for the SCMS, detailed below, focused primarily on organizational connections and separations, as well as the closely-related process of characterizing functions as

"central" or "non-central" (which is intimately tied to the issue of system ownership and operation). It also examined the cost, security risk, and operational/policy implications of the different SCMS models.

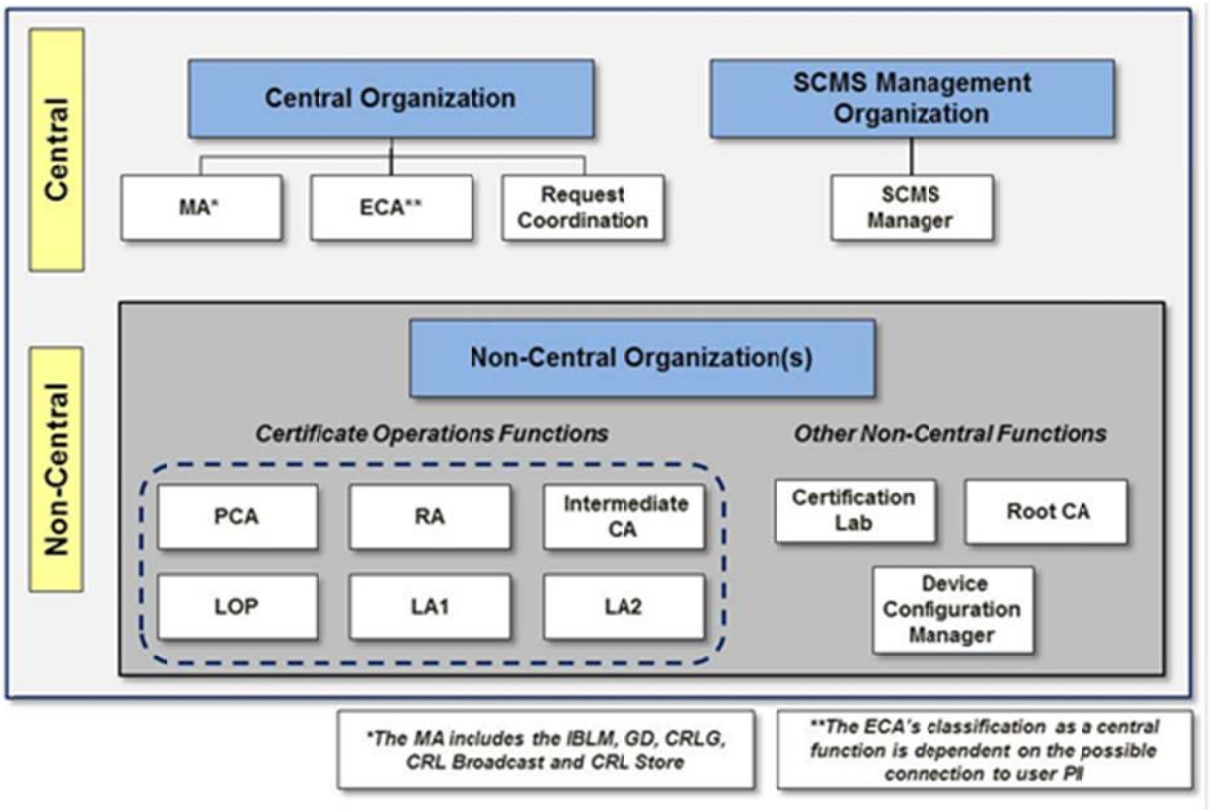
BAH began by identifying multiple organizational models that, together, captured all possible configurations of the SCMS functions identified by CAMP. DOT initially selected a small number of these organizational models for BAH to further consider. As CAMP's technical design evolved, DOT instructed BAH to reconfigure the models to reflect additional SCMS functions added to the SCMS design by CAMP, as well as CAMP's new categorization of functions as either "central" or "non-central." Based on its independent PKI research, as well as new insights into the security design communicated by CAMP, BAH then simplified the initial organizational design proposed by CAMP to remove certain organizational separations of functions that BAH determined were not necessary for security or privacy reasons.

Ultimately, the organization of the SCMS – the final grouping of functions and estimates of any efficiencies -- will be controlled by the organization(s) that manage the SCMS and own and operate the component CMEs. However, NHTSA and DOT anticipate being able to influence the organization and operation of the SCMS (and thereby ensure adequate separation to assure secure, privacy-appropriate V2V communications) through an agreement or MOU with the SCMS Manager and/or through participation on a SCMS "governance board."

BAH's SCMS organizational model/analysis, Figure 2, is based on CAMP's current SCMS technical design and represents BAH's perspective of how functions within the SCMS may be grouped.

[GPO – PHOTO GRAPHIC]

Figure 2 Security Certificate Management System Organizational Model



[END PHOTO]

Organizational separation of functions is an example of a policy control often used to mitigate privacy risks in PKI systems – but such separations come with increased costs and may negatively impact the system's ability to identify and revoke the credentials of misbehaving devices. Ultimately, more than one function may be co-located within the same SCMS component organization. However, grouping of SCMS functions and any resulting efficiencies/risk trade-offs will depend, in large part, on: (1) the system's ownership, operational structure, and governance in accordance with DOT, and (2) the preferences of the entity or entities that own and operate the SCMS Manager and CME component entities.

The SCMS Manager is intended to serve as the entity that provides system management, primarily by enforcing and auditing compliance with uniform technical and policy standards and guidance for the SCMS system-wide. The uniform standards/guidance will need to establish and ensure consistency, effectiveness, interoperability, and appropriate security and privacy protection across the CMEs, in order to facilitate necessary communications, sharing of information, and operational connections. The SCMS Manager will need to have mechanisms to ensure that all CME entities have policies, practices, technologies, and communications consistent with system-wide standards and guidance. The SCMS Manager may (but need not) be the body that develops the standards, guidance, or policies applicable system-wide; however, it would be the entity charged with overseeing standards and policy compliance by the CME entities that, together with the SCMS Manager, make up the SCMS. The agency anticipates existing PKI technical standards and industry best practices likely will form the basis for many of the policies and procedures applicable across the SCMS.[6]

VI. The Legal Relationship between NHTSA and the SCMS

As currently envisioned by NHTSA, deployment of V2V technologies requires existence of an SCMS to provide necessary security functions. In its February 3, 2014, announcement, NHTSA expressed its intent to begin working on a regulatory proposal to require V2V devices in new motor vehicles in a future year, and on August 18, 2014, NHTSA announced an advance notice of proposed rulemaking to start the regulatory process for V2V technology. A subsequent NHTSA V2V regulatory proposal, a notice of proposed rulemaking (NPRM), potentially could

[6] BAH SCMS Design and Analysis Report, at 29.

extend to many aspects of the hardware, software, and communications, making up significant parts of the V2V system. However, NHTSA, at this time, anticipates that establishment of the SCMS itself, which will provide security services necessary for secure reliable V2V messaging within the V2V system, will not be encompassed in its regulatory proposal. Instead, as discussed elsewhere in today's RFI, NHTSA envisions that constitution and operation of the SCMS will be undertaken by one or more private entities, working collaboratively with NHTSA. NHTSA and DOT do not currently envision the Federal government being the owner or operator of the SCMS.

There is a wide range of collaborative relationships that NHTSA potentially could enter into with the private entity or entities that manage or make up the SCMS. The overarching goal of the relationship(s) would be to ensure the existence and operation of an SCMS needed to support the V2V system in a way that appropriately protects consumer privacy and system security and does not impose inordinate costs on OEMs, vehicle drivers, or others. Ultimately, the nature and scope of the relationship(s) will turn on the specific terms upon which the parties agree.

Section IV of the research report contains discussion of the agency's authority to enter into agreements documenting the collaborative relationship between NHTSA and the private entity or entities that constitute and operate the SCMS supporting V2V communications. As discussed for the first time in this RFI, such an agreement would likely address or provide minimum requirements in the following areas:

- Service Period: How long the entity or entities would commit to ensuring availability of security services required to support the V2V system;

- Organization: Legal/administrative separation between, and the legal relationship among, CMEs that make up the SCMS;
- Operation: Certificate, security, privacy, audit, interoperability, and related operational policies;
- Governance: Initially, and on an ongoing basis, transparent mechanisms for obtaining input on issues relevant to SCMS constitution and operation from (1) the CMEs that make up the SCMS and (2) other stakeholders;
- System Access: To ensure support for V2V, V2I, and V2X applications and users (consumers and manufacturers) in the U.S., Canada and Mexico;
- Fees: Service and user classes for V2V, V2I, and V2X users (consumers and manufacturers);
- Privacy: Controls, enforcement, reporting (internal and to NHTSA), and data policies that provide clear notice to consumers of (among other things) what data is being collected, how it is used, and, for opt-in services, giving consumers control over access to their data;
- Security: Controls, enforcement, and reporting (internal and to NHTSA);
- Continuity of Operation: Procedural mechanisms to ensure continued support for the V2V system;
- Liability/Insurance: Liability and business interruption insurance;

- Cooperation: Procedures for working with Federal and State law enforcement and consumer fraud authorities to address any issues that threaten the system's safety or security.

VII. Specific Questions for this Notice

Specific questions posed in this notice follow. Respondents are reminded that feedback on any aspects of this notice is welcome from all interested public, private, and academic entities. If your responses relate to *how* NHTSA should implement a requirement for V2V, and the agency's authority to require V2V, rather than to the SCMS issues outlined in this notice, please submit such responses as comments to the rulemaking docket for the ANPRM (NHTSA-2014-0022) rather than this docket. While all feedback regarding the agency's regulatory announcements and the ANPRM is welcome from all parties, NHTSA is particularly interested, regarding this request for information, in hearing from those entities interested in establishing an SCMS. Respondents may respond, to some, all, or none of these specific questions:

1. SCMS ownership and operation are inextricably linked to SCMS governance. DOT research to date has focused on the likelihood of private ownership and operation of the SCMS "industry," with governance being largely "self-governance" by private industry participants and stakeholders. Other basic organizational models that could apply, besides this private model, are: public, and public-private. What model is most appropriate and what are the risks, if any, associated with a private "self-governance" approach and how would you mitigate them?

2. The SCMS has many functions that are needed to establish the trusted environment required for V2V communications. The SCMS consists of both central and non-central functions to be carried out by legally distinct CMEs that can be owned and operated by

various individual entities. What is your interest in helping to establish an SCMS? Which SCMS functions are you most interested in performing, either on your own or as part of a larger consortium? What information or other resources do you need to initiate planning, development, and implementation of the identified SCMS functions? The agency would also appreciate respondents providing potential lead times associated with standing up an SCMS and making it fully operational to support a national implementation of V2V technology, because lead time will help the agency understand when V2V technology could potentially be rolled out most successfully.

3. In relation to the SCMS Manager function, will the establishment of either a binding or non-binding "governance board" provide the appropriate level of stakeholder guidance and direction to facilitate a viable and self-sustaining business entity? If not, why not, and what additional or other type of governance or oversight might be needed?

4. In order for the SCMS to function, what standards and policies applicable to individual CMEs will need to be developed and implemented? Who do you envision will establish the various standards, policies, procedures, auditing processes, and other related industry-wide processes?

5. NHTSA and DOT anticipate being able to influence the organization and operation of the SCMS (and thereby ensure adequate separation to assure secure, privacy appropriate V2V communications) through some type of agreement with the SCMS Manager or through participation on an SCMS "governance board." In the "Legal Relationship between NHTSA and the SCMS" section of this Request for Information, we identify some likely components of an agreement between NHTSA and the SCMS Manager or entities making up the SCMS. Are there other components that such an agreement

should cover? If so, please identify them and explain their importance. If the SCMS established a "governance board," how should the board be constituted? Should the board's decisions be binding on the SCMS? Typically, NHTSA and other Federal government entities participate as non-voting liaisons or ex officio members of private boards (NHTSA, for example, regularly assigns agency employees to be non-voting liaisons on Society of Automotive Engineers (SAE) and Transportation Research Board (TRB) Committees and Boards). Would it be viable for NHTSA to participate in this manner?

6. The agency asks respondents to provide their projections of initial capital investment for SCMS functions overall and components they may potentially be interested in "standing up" and supporting.

7. Additionally, the agency welcomes feedback on how respondents envision SCMS financial sustainability and its relation to any data collection or fees, if any, that would be permitted under the agreement with DOT.

8. If you are interested in performing certain functions related to the SCMS, explain how you would ensure that privacy concerns are addressed in performance of those functions.

Authority: 49 U.S.C. 30101 et. seq.; 49 CFR part 1.95.

Issued in Washington.

Daniel C. Smith,
Senior Associate Administrator for Vehicle Safety.

Billing Code 4910-59-P

[FR Doc. 2014-24482 Filed 10/14/2014 at 8:45 am; Publication Date: 10/15/2014]